can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) All carriers shall maintain a record, electronically or in some other manner, of their sales and marketing campaigns that use CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, the date and purpose of the campaign, and what products or services were offered as part of the campaign. Carriers shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999]

EFFECTIVE DATE NOTE: At 64 FR 53264, Oct.1, 1999, §64.2009 was amended by revising paragraphs (a), (c), and (e). These paragraphs contain information collection and recordkeeping requirements and will not become effective until approval has been given by the Office of Management and Budget.

Subpart V—Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act (CALEA)

SOURCE: 64 FR 51469, Sept. 23, 1999, unless otherwise noted.

§ 64.2100 Purpose.

Pursuant to the Communications Assistance for Law Enforcement Act, Public Law 103–414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.), this subpart contains rules that require a telecommunications carrier to ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with appropriate legal authorization, appropriate carrier authorization, and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.

§ 64.2101 Scope.

The definitions included in this subchapter shall be used solely for the purpose of implementing CALEA requirements.

§ 64.2102 Definitions.

(a) *Appropriate legal authorization*. The term *appropriate legal authorization* means:

(1) A court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications; or

(2) Other authorization, pursuant to 18 U.S.C. 2518(7), or any other relevant federal or state statute.

(b) *Appropriate carrier authorization*. The term *appropriate carrier authorization* means the policies and procedures adopted by telecommunications carriers to supervise and control officers and employees authorized to assist law

enforcement in conducting any interception of communications or access to call-identifying information.

(c) *Appropriate authorization*. The term *appropriate authorization* means both appropriate legal authorization and appropriate carrier authorization.

§ 64.2103 Policies and procedures for employee supervision and control.

A telecommunications carrier shall:

(a) Establish policies and procedures to ensure the supervision and control of its officers and employees;

(b) Appoint a senior officer or employee as a point of contact responsible for affirmatively intervening to ensure that interception of communications or access to call-identifying information can be activated only in accordance with appropriate legal authorization, and include, in its policies and procedures, a description of the job function of the appointed point of contact for law enforcement to reach on a seven days a week, 24 hours a day basis;

(c) Incorporate, in its polices and procedures, an interpretation of the phrase *appropriate authorization* that encompasses the definitions of *appropriate legal authorization* and appropriate carrier authorization, as stated above;

(d) State, in its policies and procedures, that carrier personnel must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call-identifying information;

(e) Report to the affected law enforcement agencies, within a reasonable time upon discovery:

(1) Any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities; and

(2) Any act of unlawful electronic surveillance that occurred on its premises.

(f) Include, in its policies and procedures, a detailed description of how long it will maintain its records of each interception of communications or access to call-identifying information pursuant to § 64.2104.

[64 FR 51469, Sept. 23, 1999, as amended at 64 FR 52245, Sept. 28, 1999]

EFFECTIVE DATE NOTE: At 64 FR 51469, Sept. 23, 1999, § 64.2103 was added, and at 64 FR 52245, Sept. 28, 1999, it was amended by revising paragraph (f). This section contains information collection and recordkeeping requirements and will not become effective until approval has been given by the Office of Management and Budget.

§ 64.2104 Maintaining secure and accurate records.

(a) A telecommunications carrier shall maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certification.

(1) This certification must include, at a minimum, the following information:

(i) The telephone number(s) and/or circuit identification numbers involved;

(ii) The start date and time of the opening of the circuit for law enforcement;

(iii) The identity of the law enforcement officer presenting the authorization;

(iv) The name of the person signing the appropriate legal authorization;

(v) The type of interception of communications or access to call-identifying information (e.g., pen register, trap and trace, Title III, FISA); and

(vi) The name of the telecommunications carriers' personnel who is responsible for overseeing the interception of communication or access to call-identifying information and who is acting in accordance with the carriers' policies established under § 64.2103.

(2) This certification must be signed by the individual who is responsible for overseeing the interception of communications or access to call-identifying information and who is acting in accordance with the telecommunications carrier's policies established under § 64.2103. This individual will, by his/her signature, certify that the record is complete and accurate.

(3) This certification must be compiled either contemporaneously with, or within a reasonable period of time